REMARKS/ARGUMENTS

The Examiner's objection to Claim 9 has been overcome by reciting --said digital data-- as suggested by the Examiner.

Claims 1-12 have been rejected under 35 U.S.C. 112. Claim 1 has been amended to recite "an identification" as suggested by the Examiner.

Claim 9 has been amended to specifically recite which system is being recited.

Claim 9 has been amended to specifically recite which detection means is recited.

Claim 9 has been amended to specifically recite which protection system is being recited.

Claim 9 has been amended to recite "said digital data" so as to overcome the Examiner's objection.

In order to overcome the Examiner's objection to Claim 1 under 35 U.S.C. 101, Claim 1 has been amended to recite a method of protection against the copying of digital data stored on a storage medium.

Claim 1 has been rejected under 35 U.S.C. 102(e) as being anticipated by Linnartz U.S. Patent 6,314,518. Nowhere does Linnartz show or suggest a step of identifying whether digital data stored on a storage medium is encrypted, as specifically recited in Claim 1 as amended. The Examiner has referred to column 4, lines 1-19 and column 5, lines 30-47 of Linnartz. However, nothing in these cited portions of Linnartz teaches or suggests detection of encryption. The Applicants therefore submit that the amendment to Claim 1 overcomes the Examiner's rejection under 35 U.S.C. 102.

Claim 1 and its subclaims have been rejected under 35 U.S.C. 103(a) as being unpatentable over Linnartz U.S. Patent 6,314,518. In his rejection, the Examiner considers that a "hash value is obtained via a one-way encryption of data" and deduces from the assertion that Linnartz teaches an encryption of digital data. In fact, "hash functions" are one-way functions which take a message as input and produce an output of fixed length. Such hash code can not be equated with encryption of data, which aims at rendering data unintelligible in a reversible way. For example, when data is

encrypted, it is, in principle, possible to decrypt it if one has the necessary decryption key. On the other hand, a hash code can not be decrypted. In addition, even if Linnartz mentions, in some parts of the document, the encryption of data, it is only for the purpose of securing a link between an MPEG decoder and a disc drive. See column 8, lines 49-50. Linnartz fails to disclose a step of identifying (i.e., detecting) whether data are encrypted, and then a step of authorizing or prohibiting copy or playback of the data depending on the result of this identification (in combination with the additional detection of watermark in the data).

The Examiner indicates that the different embodiments disclosed in the Linnartz reference could be combined to obtain the present invention. However, nowhere does Linnartz show or suggest a method of protection against copying of digital data stored on a storage medium, the method comprising:

identifying whether said digital data are encrypted;

identifying whether said digital data are watermarked; and

delivering one of a permission and a prohibition to copy and/or to play the digital data as a function of the identification of:

an encryption of said digital data; and

a watermarking of said digital data,

as specifically set forth in Claim 1.

It is therefore clear that nowhere does Linnartz show or suggest any information which could be used to derive the method set forth in Claim 1 as amended.

Claim 9 has been rejected under 35 U.S.C. 103(a) as being unpatentable over Linnartz in view of Ichinoi U.S. Patent 6,266,477. Nowhere does Linnartz show or suggest:

means for detecting whether said digital data are encrypted;

a system for protection against copying which is able to generate a copy permission signal or a copy prohibition signal as a function of the signals received from said means for detecting (including means for detecting whether said digital data are watermarked), means for detecting whether a storage medium is recordable, means

for detecting whether said storage medium contains a cryptographic signature accompanying the digital data; and

a system for protection against playing being able to generate a playing prohibition signal when it has been detected by said means for detecting that said digital data are not encrypted and that said digital data are watermarked,

as specifically recited in Claim 9.

The Examiner points out that Linnartz "is only worried about copy/play control via the use of watermarks, and not encryption of the data at all. Therefore, a playing signal would be generated based on an encryption of the digital data not being detected and based on the watermarking of the digital data". The Applicants submit that Claim 9 as amended recites that the play and prohibition signal is generated when the means for detecting detects that the digital data are not encrypted and that the digital data are watermarked. This is not taught or suggested by Linnartz. Rather, Linnartz teaches only one detection being performed (watermark detection) and where the content of the watermark detected (watermark state (a), (b), (c) or (d) determines whether the playback of the content is allowed or not. See column 5, lines 4-10 of Linnartz.) In contrast, in the instant invention it is the presence or absence of a watermark that determines, in combination with the identification of an encryption of the data, whether the play and protection system will generate a playing prohibition signal.

The cited patent to Ichinoi only discloses a descrambler 2 (after a front end section 1) in a data recording and playback system. Contrary to the Examiner's statement at the end of page 15 of the Office Action, the presence of a descrambler 2 does not imply that "the descrambler must be able to determine which signals are encrypted and which are not, to properly perform decryption on the signals". There are other possibilities such as using information contained in packet headers of the packets carrying the digital data to determine whether data should be descrambled or not. The Applicants therefore submit that Ichinoi fails to teach the recitations that are not disclosed in the Linnartz reference. Consequently the combination of these references does not render obvious the subject matter of Claim 9.

Claims 2-8 and 10-12 are dependent from Claim 1 and recite further advantageous features. The Applicants submit that these subclaims are patentable as their parent Claim 1.

The Applicants submit that the instant application is now in condition for allowance. A notice to that effect is respectfully solicited.

The Applicants believe that no fee, in addition to the fee for a three-month extension, is believed due. However, if a fee is due, the Applicants request that any additional fee be charged to Deposit Account 07-0832.

Respectfully submitted,
Sylvain Chevreau et al.

By: Catherine A Ferguson
Catherine A. Ferguson
Reg. No. 40,877
Tel. No. (609)734-6440

Thomson Licensing Inc.
Patent Operations
PO Box 5312
Princeton, NJ 08543-5312
15 May 2006